PATENT APPLICATION
Docket No. MS1-775US

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of		)
		)
	Mitchell et al	)
		)
Serial No.:	09/836,584	) Appeal No.
		)
Confirmation No.	7869	)
		)
Filed:	April 16, 2001	)
		)
For:	Methods and Arrangements for Selectively Maintaining Parental Access Consent in a Network Environment	)))
		)
Examiner:	Truong, Thaninga B.	)

The Honorable Commissioner of Patents
Mail Stop Appeal Brief - Patents
P.O. BOX 1450
Alexandria, VA 22313-1450

BRIEF OF APPELLANT

The Applicant has filed a timely Notice of Appeal from the action of the Examiner in finally rejecting all of the claims that were considered in this application. This Brief is being filed under the provisions of 37 C.F.R. § 1.192. The Filing Fee, as set forth in 37 C.F.R. § 1.17(c), is submitted herewith.

TABLE OF CONTENTS

Real Party in Interest	Page 3
Related Appeals and Interferences	Page 4
Status of Claims	Page 5
Status of Amendments	Page 6
Summary of the Claimed Subject Matter	Page 7
Grounds of Rejection to be Reviewed on Appeal	Page 10
Argument	Page 11
Claims Appendix	Page 27
Evidence Appendix	Page 36
Related Proceedings Appendix	Page 37

REAL PARTY IN INTEREST

The real party in interest is Microsoft Corporation, by way of assignment from Mitchell et al., who is the named inventive entity and is captioned in the present brief.

RELATED APPEALS AND INTERFERENCES

None.

STATUS OF CLAIMS

Claims 1-47 are pending in the application and stand finally rejected by the Examiner.

STATUS OF AMENDMENTS

None.

SUMMARY OF THE CLAIMED SUBJECT MATTER

Beginning at page 9 of the subject Application, an example of the use of consent information is described. Consent information is obtained from a first party, where such information allows a second party access to a network server that requires such consent information to access the server. After initially obtaining the consent information, the obtained consent information can then be stored, for example, in a user profile of the second party. The user profile is a collection of information that may include information such as, for example, the user's name, password, email address, personal preferences and/or various other information about the user.

Once the consent information has been stored in the user profile of the second party, the second party may then access the network server and network facilities, such as for example, web sites operated in conjunction with the network server for which consent has been given. By way of example, the first party may modify the consent information through his/her own user profile. In this manner, a user profile of the first party is created and logically linked to the user profile of the second party. This allows the first party to access and modify such consent information stored in the user profile of the second party via the user profile of the first party.

At pages 23-24 of the subject application, it is made apparent that certain provisions in the Child's Online Privacy Protection Act (COPPA) require that parent be allowed to access and possibly modify any data collected by the child, such as to access and edit a user profile of the child and also any addition information collected with regard to the child. With this in mind, a validation protocol or validation code may be built to work in conjunction with or as part of authentication processes. For instance, the validation code may be sent from an authentication server to an affiliate server to allow the receiving affiliate server to know which child record a parent wishes to access and/or possibly modify. Thus, the validation code does not require the affiliate server and/or client computer system to determine know or otherwise store any record of the applicable parent child relationship.

Independent claim 1 recites a method comprising "associating a first entity with a second entity in a first device" and "selectively providing information about the association of the first and second entities to a second device as directed by the first entity, without requiring the second entity to be operatively associated with either the first or second device" (page 24, line13 to page 25, line 6).

Independent claim 12 recites a computer-readable medium having computer-executable instructions, comprising: "associating a first entity with a second entity in a first device" and "causing the first device to selectively provided information about the association of the first and second entities to a second device when directed by the first entity, without requiring the second entity to be operatively associated with either the first or second device" (page 24, line13 to page 25, line 6).

Independent claim 23 recites an apparatus comprising "memory having information associating a first user of the apparatus with a second user of the apparatus" and "logic operatively coupled to the memory and configured to respond to inputs from the first user by selectively outputting the information about the association of the first user and the second user, without requiring the second user to be operatively signed-in to the apparatus" (page 24, line13 to page 25, line 6).

Independent claim 32 recites a computer-readable medium having stored thereon a data structure, comprising "a validation code that identifies a first entity and a second entity" (page 24, line13 to page 25, line 6).

Independent claim 37 recites an apparatus comprising memory and "logic operatively coupled to the memory and configured to allow a first entity to be operatively associated with the apparatus, and receive information about an association of the first entity and at least one other entity, without requiring the at least one other entity to be operatively associated with the apparatus" (page 24, line13 to page 25, line 6).

GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

1. Whether Claims 1-3, 8, 10-14, 19, 21-23, 28, 30-31, 37-39, 44 and 46-47 were properly rejected under 35 U.S.C. § 102(b) as being anticipated by U.S. Patent No. 5,678,041 to Baker et al. (hereinafter "Baker").

2. Whether Claims 4-7, 15-18, 24-27, 32-36 and 40-43 were properly rejected under 35 U.S.C. § 102(e) as being anticipated by Baker.

3. Whether Claims 9, 20, 29 and 45 were properly rejected under 35 U.S.C. § 102(e) as being anticipated by Baker.

ARGUMENT

First Ground of Rejection. Claims 1-3, 8, 10-14, 19, 21-23, 28, 30-31, 37-39, 44 and 46-47 satisfy the requirements of 35 U.S.C. § 102(b) and therefore are not anticipated by Baker.

1. **Baker describes a Rating System by Network Managers to Restrict User Access**

Baker describes a system and method for restricting user access rights on the Internet based on rating information stored in a relational database. Baker describes that "there exists no simple means for an authority (i.e., teacher, supervisor, system administrator, etc.) to selectively control WWW access by one or more users without significantly impairing the user's ability to communicate with the Internet." *See Baker, Col. 2, Line 66 to Col. 3, Line 3.* To provide this control, Baker describes a rating system "that allows one or more network administrators/managers to rate particular information and/or services", the rating is utilized "to restrict specific system users from accessing the information/service via certain public or otherwise uncontrolled databases". *See Baker, Col. 3, Lines 11-14.* Baker then describes a "relational database [which] is arranged so that for each user of the system a request for a particular resource will only be passed on from the local network to a server providing a link to the public/uncontrolled database if the resource identifier has an access rating for which the user has been assigned specific permissions by an administrator/manager". *See Baker, Col. 3, Lines 21-29.* Therefore, although Baker discloses a network administrator as being able to control access of other users, Baker does not disclose, teach or suggest selectively providing information <u>about the association</u> nor about associating first and second entities in a first device.

2. <u>Applicant describes Selectively Providing Consent Information About an Association of First and Second Entities as directed by the First Entity</u>

Beginning at page 9 of the subject Application, an example of the use of consent information is described. Consent information is obtained from a first party, where such information allows a second party access to a network server that requires such consent information to access the server. After initially obtaining the consent information, the obtained consent information can then be stored, for example, in a user profile of the second party. The user profile is a collection of information that may include information such as, for example, the user's name, password, email address, personal preferences and/or various other information about the user.

Once the consent information has been stored in the user profile of the second party, the second party may then access the network server and network facilities, such as for example, web sites operated in conjunction with the network server for which consent has been given. By way of example, the first party may modify the consent information through his/her own user profile. In this manner, a user profile of the first party is created and logically linked to the user profile of the second party. This allows the first party to access and modify such consent information stored in the user profile of the second party via the user profile of the first party.

Certain provisions in the Child's Online Privacy Protection Act (COPPA) require that parent be allowed to access and possibly modify any data collected by the child, such as to access and edit a user profile of the child and also any addition information collected with regard to the child. With this in mind, a validation protocol or validation code may be built to work in conjunction with or as part of authentication processes. For instance, the validation code may be sent from an authentication server to an affiliate server to allow the receiving affiliate server to know which child record a parent wishes to access and/or possibly modify. Thus, the validation code does not require the affiliate server and/or client computer system to determine, know or otherwise store any record of the applicable parent child relationship.

3. **Claims 1-3, 8, 10-14, 19, 21-23, 28, 30-31, 37-39, 44 and 46-47 are not anticipated by Baker**

In each of the responses to the Office Actions filed by the Applicant, the Applicant respectfully requested clarification of rejections which the Applicant asserted were unclear. Applicant respectfully maintains that it is unclear which portions of Baker the Examiner is relying upon as a basis for the features recited in claim 1, as well as the other claims. As is "well settled", "[w]here a major technical rejection is proper, it should be stated with a full development of reasons rather than by a mere conclusion coupled with some stereotyped expression." MPEP. §707.07(g). Further, MPEP § 706 refers to C.F.R § 1.104 which describes the required specificity of claim rejections in the following excerpt:

> In rejecting claims for want of novelty or for obviousness, it is well settled that the Examiner must cite the best references at his or her command. When a reference is complex or shows or describes inventions other than that claimed by the applicant, the particular part relied on must be designated as nearly as practicable. The pertinence of each reference, if not apparent, must be clearly explained and each rejected claim specified. 37 C.F.R. 1.104(c)(2).

The Examiner's Action is almost entirely composed of direct claim language coupled with bare, unexplained references to and excerpts from Baker. No particular explanation of Baker is offered. For example, it is entirely unclear what the Examiner is asserting for a first entity, a second entity, or for an association between first and second entities. Accordingly, as is addressed in detail in the following remarks, Applicant asserts that a *prima facie* case of anticipation has not been established and that the §102 rejection should be overturned.

Claim 1 recites a method which includes "associating a first entity with a second entity in a first device" and "selectively providing information about the association of the first and second entities to a second device as directed by the first entity, without requiring the second entity to be operatively associated with either the first or second device". **Claim 12** recites a computer-readable medium which includes "associating a first entity with a second entity in a first device" and "causing the first device to selectively provide information about the association of the first and second entities to a second device as directed by the first entity, without requiring the second entity to be operatively associated with either the first or second device". **Claim 23** recites an apparatus having "memory having information associating a first user of the apparatus with a second user of the apparatus" and "logic operatively coupled to the memory and configured to respond to inputs from the first user by selectively outputting the information about the association of the first user and the second user, without requiring the second user to be operatively signed-in to the apparatus". **Claim 37** recites an apparatus having "memory" and "logic operatively coupled to the memory and configured to allow a first entity to be operatively associated with the apparatus, and receive information about an association of the first entity and at least one other entity, without requiring the at least one other entity to be operatively associated with the apparatus". To simplify the following discussion, claim 1 will be argued with the arguments being equally applicable to claims 12, 23 and 37.

The Examiner first asserts that the "associating" as recited above is described in Baker at column 3, lines 60-65, the portion of which is excerpted as follows:

> As shown in FIG. 1, the system includes public network 100, network resources 101-105, and user site 106. Particular users at user site 106 gain access to public network 100 via user terminals 107, 108 and 109. Each of these user terminals is linked by local area network ("LAN") 110 to processor 111 within proxy server 112. *Baker, Col. 3, Lines 60-65.*

As shown in the above referenced portion, Baker merely describes user terminals linked by a local area network. The Examiner makes no indication of what in the above recited portion is relied upon for the features of claim 1.

In response to Applicant's remarks in the Response filed 1/24/2005, the Examiner further asserts Baker column 4, lines 1-16, (Office Action dated 5/13/2005 p. 6-7) the portion of which is excerpted as follows:

> Requests from user terminals 107-109 for access to network resources (101-105) through public network 100 are submitted to processor 111 within proxy server 112. In this particular embodiment of the invention, the submitted requests are assumed to be in the form of URLs. As is well known in art, when URLs are submitted to a proxy server, the particular requesting user terminal is identified to the proxy server by an identification header attached to the URL. For the system shown in FIG. 1, the identification code for user terminal 107 is ID.sub.107, the identification code for user terminal 108 is ID.sub.108, and the identification code for user terminal 109 is ID.sub.109. In addition, within the system of FIG. 1, URLs designated as URL.sub.101, URL.sub.102, URL.sub.103, URL.sub.104 and URL.sub.105, represent requests for information from network resources 101, 102, 103, 104 and 105, respectively. *Baker, Col. 4, Lines 1-16.*

As shown in the above referenced portion, Barker describes requests in the form of URLs submitted to a proxy server. These URLs may be used to identify the requesting user terminal. The above referenced portion does not clarify what particular components of Baker are relied upon. Further, no attempt is made to clarify the rejection in light of the cited portion. Only the portion itself is offered. Neither the Examiner nor the cited portion describes any association between entities. Applicant asserts that the cited portions of Baker provides no basis for "associating a first entity with a second entity in a first device" as recited in claim 1.

The Examiner next asserts that "selectively providing" as recited above is described in Baker at column 5, lines 45-65, the portion of which is excerpted as follows:

> In the particular embodiment described above, relational database 114 stores a list of user terminal identification codes and the various user clearances reflective of the ratings of network resources that each user terminal should be allowed to retrieve from public network 100. It will be understood that the invention could be modified so that the list of user clearances associated with a given user terminal identification code serves as a restrictive list (i.e.; that user is not allowed to retrieve network resources having that rating). This restrictive listing functionality could be readily facilitated by reprogramming processor 111. In addition, the invention could be modified so that the identification codes recognized by processor 111 and stored in relational database 114 are user specific, as opposed to user terminal specific. In other words, the system of FIG. 1 could be modified so that a given individual using a terminal is identified to the system by a personal password or other identifying code. Access or denial of the transmission of particular URLs is effected by the system as a function of that

> person's identity, regardless of the particular user terminal they may be utilizing. *Baker, Col. 5, Lines 45-65.*

As show in the above referenced portion, Baker merely describes using user specific identification codes so that access or denial of a transmission from a particular URL is a function of that user's identity. It is respectfully submitted that the Examiner has misinterpreted the language of Claim 1.

In response to Applicant's remarks in the Response filed 1/24/2005, the Examiner further asserted Baker column 4, lines 7-35, (Office Action dated 5/13/2005 p. 7), the portion of which is excerpted as follows:

> Upon receipt of an incoming URL, processor 111 is programmed to determine the identity of the requesting user terminal from the URL header. This identification information is then utilized by processor 111 to cross-reference the received URL with information stored in relational database 114. Relational database 114 contains listing 115 which associates each of the user identification codes (ID.sub.107, ID.sub.108 and ID.sub.109) with a user clearance code (user clearances.sub.107, user clearances.sub.108 and user clearances.sub.109, respectively). These user clearances indicate the particular rating class or classes of network resources that a given user terminal is allowed to access (i.e.; unlimited access; restricted use of URLs identified as accessing violent subject matter; restricted use of URLs that are identified as accessing obscene subject matter; etc). Also contained in relational database 114 is listing 116 which includes a register of allowable URLs (URL.sub.101-105) that may be transmitted from a user terminal to access network resources. *Baker, Col. 4, Lines 17-35.*

As shown in the above referenced portion, Barker describes that processor 111 identifies the requesting user terminal. This user terminal id may be used to cross-reference the URL with database information. Baker merely uses a URL request to cross reference the requesting user terminal with the particular clearance code for that user terminal. Each user id and clearance id are associated with a particular user terminal. Baker does not disclose an association of or selectively providing information about an association of user terminals. Again, the above referenced portion does not clarify what particular components of Baker the Examiner is relying upon. Further, no attempt is made to clarify the rejection in light of the cited portion. Applicant asserts that the cited portions of Baker provide no basis for "selectively providing information about the association of the first and second entities to a second device" as recited in claim 1.

Further, Baker fails to describe "providing information about the association of a first and second entity to a second device as directed by the first entity" or "without requiring the second entity to be operatively associated with either the first or second device" which are additional recited features of claim 1. The Office relies upon the passages excerpted above for these additional features of claim 1. Baker does not disclose these recited features in the portions cited by the Examiner, or elsewhere.

To anticipate a claim, the reference must teach every element of the claim. *MPEP § 2131.* A claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference." *Verdegaal Bros. v. Union Oil Co. of California*, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987). Here, Baker fails to disclose each and every claim limitation. Baker does not disclose, teach or suggest "associating a first entity with a second entity in a first device" as recited in Claim 1. Rather, the referenced portions of Baker merely describe user terminals linked by a local area network. Further, Barker does not disclose, teach or suggest "selectively providing information about the association of the first and second entities" as recited in Claim 1. Baker fails to even mention information about an association in the portions relied upon by the Examiner, nor elsewhere in the asserted reference. Baker further fails to disclose, teach, or suggest "providing information about the association of a first and second entity to a second device as directed by the first entity" or "without requiring the second entity to be operatively associated with either the first or second device". Therefore, it is respectfully submitted that a *prima facie* case of anticipation has not been established.

Claims 2-11 depend either directly or indirectly from claim 1 and are allowable as depending from an allowable base claim. **Claims 13-22** depend either directly or indirectly from Claim 12 and are allowable as depending from an allowable base claim. **Claims 24-31** depend either directly or indirectly from Claim 23 and are allowable as depending from an allowable base claim. **Claims 38-47** depend either directly or indirectly from Claim 37 and are allowable as depending from an allowable base claim. These claims are also allowable for their own recited features which, in combination with those recited their respective independent claims, are neither shown nor suggested in the references of record, either singly or in combination with one another, examples of which are described in relation to the Second and Third Grounds of Rejection.

The Applicant respectfully requests that the Board overturn the First Ground of Rejection.

Second Ground of Rejection. Claims 4-7, 15-18, 24-27, 32-36 and 40-43 satisfy the requirements of 35 U.S.C. § 102(b) and therefore are not anticipated by Baker.

Claim 32 recites "a computer-readable medium having stored thereon a data structure, comprising: a validation code that identifies a first entity and a second entity." Baker does not disclose, teach or suggest these aspects. The Office asserts that Claim 32 has "limitations that is similar to those of claim 1, thus they are rejected with the same rationale applied against claim 1 above". *Office Action Dated October 6, 2004, Page 4.* The Applicant respectfully disagrees. However, following this assertion, the Applicant submits that Claim 32 is allowable based on the reasoning offered in respect to Claim 1. Additionally, Claim 32 is also allowable based on the recitation of "a validation code that identifies a first entity and a second entity", which is not disclosed, taught or suggested by Baker. In response to Applicant's previous remarks (Response filed 1/24/2005), the Office further asserts Baker column 4, lines 17-25, (*Office Action dated 5/13/2005 p. 8*) the portion of which is excerpted as follows:

> Upon receipt of an incoming URL, processor 111 is programmed to determine the identity of the requesting user terminal from the URL header. This identification information is then utilized by processor 111 to cross-reference the received URL with information stored in relational database 114. Relational database 114 contains listing 115 which associates each of the user identification codes (ID.sub.107, ID.sub.108 and ID.sub.109) with a user clearance code (user clearances.sub.107, user clearances.sub.108 and user clearances.sub.109, respectively). *Baker, Col. 4, Lines 17-25.*

The recited passage indicates identification of a requesting terminal and further that a listing associates each particular user id with a particular clearance code respectively. The codes and ids are matched one to one. The passage does not show "a validation code that identifies a first and a second entity. Respectfully, nothing in the recited passage discloses the recited features of claim 32. **Claims 4-7, 15-18, 24-27, 33-36 and 40-43**, either directly or indirectly, also recite a validation code and therefore are allowable based on similar reasoning.

Therefore, since Baker does not disclose a validation code, a *prima facie* case of anticipation has not been established. The Applicant respectfully requests that the Board overturn the Second Ground of Rejection.

Third Ground of Rejection. Claims 9, 20, 29 and 45 satisfy the requirements of 35 U.S.C. § 102(b) and therefore are not anticipated by Baker.

Claim 9, for example, recites "wherein the first entity is a parent/guardian of the second entity", which is not disclosed, taught or suggested by Baker. The Office asserts that the one or more network administrators/managers are the "parent guardian". This is not the case and is inconsistent with the previous assertions made by the Office. For example, if the first entity is the network administrator, there is no disclosure, teaching or suggestion in Baker for information about the association of the network administrator with another entity. In response to Applicant's previous remarks (Response filed 1/24/2005), the Office further asserts Baker column 5, lines 36-40, (*Office Action dated 5/13/2005 p. 8*) the portion of which is excerpted as follows:

> Processor 111 could also be programmed to deny all requests from user terminals for un-rated resources. This would prohibit the accessing of network resources that had not been reviewed or rated by the system administrator/manager. *Baker, Col. 5, Lines 36-40.*

The recited passage simply indicates that all requests for unrated resource may be denied. Respectfully, nothing in the recited passage discloses "wherein the first entity is a parent/guardian of the second entity" as recited in claim 9. Claims 20, 29 and 45 are allowable for similar reasons.

Accordingly, it is respectfully asserted that a *prima facie* case of anticipation has not been established. The Applicant respectfully requests that the Board overturn the Third Ground of Rejection.

CONCLUSION

The Applicant respectfully considers this application to be in condition for allowance and respectfully requests the Board to overturn the final rejection and that the Examiner pass this application to allowance.

Dated this 15th day of June, 2006.

Respectfully submitted,

WILLIAM J. BREEN, III
Attorney for Applicant
Registration No. 45,313

LEE & HAYES PLLC
421 W. Riverside Avenue, Suite 500
Spokane, WA 99201
Telephone: (509) 324-9256 (Ext. 249)
Facsimile: (509) 323-8979

APPENDIX: CLAIMS ON APPEAL

Listing of Claims:

1. (original): A method comprising:

associating a first entity with a second entity in a first device; and

selectively providing information about the association of the first and second entities to a second device as directed by the first entity, without requiring the second entity to be operatively associated with either the first or second device.

2. (original): The method as recited in Claim 1, wherein the first entity and the second entity are selected from a group of entities that includes users, organizations, companies, devices, computers, servers, computer programs, and applications.

3. (original): The method as recited in Claim 1, wherein the first entity includes a first user, the second entity includes a second user, and wherein without requiring the second entity to be operatively associated with either the first or second device includes without requiring the second user to be logged in to either the first or second device.

4. (original): The method as recited in Claim 1, wherein selectively providing information about the association of the first and second entity to the second device further includes providing the second device with a validation code that

identifies the first entity and the second entity, when the first entity is operatively associated with the second device.

5. (original): The method as recited in Claim 4, wherein the validation code identifies the second entity by an identifier and a name.

6. (original): The method as recited in Claim 5, wherein the validation code identifies modifications to a consent parameter associated with the second entity.

7. (original): The method as recited in Claim 4, wherein providing the second device with the validation code further includes encrypting at least a portion of the validation code.

8. (original): The method as recited in Claim 1, wherein associating the first entity with the second entity in the first device further includes logically associating a first entity profile with a second entity profile.

9. (original): The method as recited in Claim 3, wherein the first entity is a parent/guardian of the second entity.

10. (original): The method as recited in Claim 1, wherein the first device includes a network server that is configured to act as an authentication server.

11. (original): The method as recited in Claim 10, wherein the second device includes a network server that is configured to act as an affiliated server associated with the authentication server.

12. (original): A computer-readable medium having computer-executable instructions, comprising:

associating a first entity with a second entity in a first device; and

causing the first device to selectively provided information about the association of the first and second entities to a second device when directed by the first entity, without requiring the second entity to be operatively associated with either the first or second device.

13. (original): The computer-readable medium as recited in Claim 12, wherein the first entity and the second entity are selected from a group of entities that includes users, organizations, companies, devices, computers, servers, computer programs, and applications.

14. (original): The computer-readable medium as recited in Claim 12, wherein the first entity includes a first user, the second entity includes a second user, and wherein without requiring the second entity to be operatively associated with either the first or second device includes without requiring the second user to be logged in to either the first or second device.

15. (original): The computer-readable medium as recited in Claim 12, wherein causing the first device to selectively provide information about the association of the first and second entities to the second device further includes providing the second device with a validation code that identifies the first entity and the second entity, when the first entity is operatively associated with the second device.

16. (original): The computer-readable medium as recited in Claim 15, wherein the validation code identifies the second entity by an identifier and a name.

17. (original): The computer-readable medium as recited in Claim 16, wherein the validation code identifies modifications to a consent parameter associated with the second entity.

18. (original): The computer-readable medium as recited in Claim 15, wherein causing the first device to provide the second device with the validation code further includes encrypting at least a portion of the validation code.

19. (original): The computer-readable medium as recited in Claim 12, wherein associating the first entity with the second entity in the first device further includes logically associating a first entity profile with a second entity profile.

20. (original): The computer-readable medium as recited in Claim 14, wherein the first user is a parent/guardian of the second user.

21. (original): The computer-readable medium as recited in Claim 12, wherein the first device includes a network server that is configured to act as an authentication server.

22. (original): The computer-readable medium as recited in Claim 21, wherein the second device includes a network server that is configured to act as an affiliated server associated with the authentication server.

23. (original): An apparatus comprising:

memory having information associating a first user of the apparatus with a second user of the apparatus; and

logic operatively coupled to the memory and configured to respond to inputs from the first user by selectively outputting the information about the association of the first user and the second user, without requiring the second user to be operatively signed-in to the apparatus.

24. (original): The apparatus as recited in Claim 23, wherein the logic is configurable to be operatively connected to at least one external device and is further configured to selectively output the information within a validation code that identifies the first user and the second user, when the first user signs-in to the external device.

25. (original): The apparatus as recited in Claim 24, wherein the validation code identifies the second user by an identifier and a name.

26. (original): The apparatus as recited in Claim 24, wherein the validation code identifies modifications to a consent parameter associated with the second user.

27. (original): The apparatus as recited in Claim 24, wherein the logic is further configured to encrypt at least a portion of the validation code.

28. (original): The apparatus as recited in Claim 23, wherein the logic is further configured logically associate a first user profile with a second user profile in the memory.

29. (original): The apparatus as recited in Claim 23, wherein the first user is a parent/guardian of the second user.

30. (original): The apparatus as recited in Claim 23, wherein the apparatus is included in a network server that is configured to act as an authentication server.

31. (original): The apparatus as recited in Claim 30, wherein the external device includes a network server that is configured to act as an affiliated server associated with the authentication server.

32. (original): A computer-readable medium having stored thereon a data structure, comprising:

a validation code that identifies a first entity and a second entity.

33. (original): The computer-readable medium as recited in Claim 32, wherein the first entity and the second entity are selected from a group of entities that includes users, organizations, companies, devices, computers, servers, computer programs, and applications.

34. (original): The computer-readable medium as recited in Claim 32, wherein the validation code identifies the second entity by an identifier and a name.

35. (original): The computer-readable medium as recited in Claim 33, wherein the validation code identifies modifications to a consent parameter associated with the second entity.

36. (original): The computer-readable medium as recited in Claim 34, wherein at least a portion of the validation code is encrypted.

37. (original): An apparatus comprising:

memory; and

logic operatively coupled to the memory and configured to allow a first entity to be operatively associated with the apparatus, and receive information about an association of the first entity and at least one other entity, without requiring the at least one other entity to be operatively associated with the apparatus.

38. (original): The apparatus as recited in Claim 36, wherein the first entity and the at least one other entity are selected from a group of entities that includes users, organizations, companies, devices, computers, servers, computer programs, and applications.

39. (original): The apparatus as recited in Claim 36, wherein the first entity includes a first user, the at least one other entity includes a second user, and wherein without requiring the at least one other entity to be operatively associated with the apparatus includes without requiring the second user to be logged in to the apparatus.

40. (original): The apparatus as recited in Claim 36, wherein the logic is configurable to receive the information about the association from an external device via a validation code that identifies the first entity and the at least one other entity, when the first entity is operatively associated with the external device.

41. (original): The apparatus as recited in Claim 39, wherein the validation code identifies the at least one other entity by an identifier and a name.

42. (original): The apparatus as recited in Claim 39, wherein the validation code identifies modifications to a consent parameter associated with the at least one other entity.

43. (original): The apparatus as recited in Claim 39, wherein the logic is further configured to decrypt the validation code, as needed.

44. (original): The apparatus as recited in Claim 39, wherein, in response to the validation code, the logic is further configurable to output previously gathered information relating to the at least one other entity to the external device.

45. (original): The apparatus as recited in Claim 38, wherein the first user is a parent/guardian of the second user.

46. (original): The apparatus as recited in Claim 36, wherein the apparatus is included in a network server that is configured to act as an affiliate server.

47. (original): The apparatus as recited in Claim 39, wherein the external device includes a network server that is configured to act as an authentication server.

EVIDENCE APPENDIX

None.

RELATED PROCEEDINGS APPENDIX

None.